Pacific University
CommonKnowledge

Volume 13 (2013)

Interface: The Journal of Education, Community and Values

12-7-2013

NSA Surveillance: How it's happening and why you should care

Paul O'Day
Berglund Student Fellow

NSA Surveillance: How it's happening and why you should care

NSA Surveillance:
How it's happening and why you should care

Editor's Note: The opinions expressed here are those of a student fellow and do not necessarily represent the opinion of Interface or the Berglund Center for Internet Studies.

By Paul O'Day
Student Fellow, The Berglund Center for Internet Studies

The government has been monitoring Internet traffic for nearly as long as the Internet has existed. By tapping Internet service providers (ISPs), they can tap the data stream before it reaches your computer. This means they have access to everything that's unencrypted, and even if the connection is encrypted, they'll still be able to tell what sites you visit. ISP monitoring can only give the government so much, however; after all, some traffic is encrypted, which is why the government also cooperates with the tech companies on the other end, like Facebook or Google, meaning they still have access to much of the encrypted data by asking the company you sent it to.

Of course, most of the details about these activities are secret—the significant information we have comes from leaks. Until recently, the fact that the NSA has programs to gather data directly from Internet companies was pure speculation, and the full extent of government monitoring is still secret. However, what information we have shows a clear disregard for the privacy of Internet users by the government. The judicial system has intervened to uphold the law on at least one occasion, and NSA officials have repeatedly lied to the public about the existence and scope of these programs, as well as about any abuses of these systems. Personnel have abused these systems, which is to be expected—every system is abused—but far too many abuses were due to a lack of proper safeguards.

Abuse and secrecy aren't the only problems with these programs. They certainly violate implied protections under the fourth amendment against unreasonable search and seizure. The government is gathering and saving a massive amount of information about its citizens' Internet habits, and it would be

possible for them to put together a file on the interests, political leanings, connections, and browsing history of any citizen that regularly uses the Internet. This would be illegal and time-consuming, and while there's no indication that the government is doing this, the capability exists.

The main law being used to justify most of this surveillance is the Foreign Intelligence Surveillance Act (FISA). Enacted in 1978 in response to illegal spying by the FBI and CIA, FISA defines who the government is allowed to spy on, under what circumstances, and the procedures for doing so. Specifically, it prevents the government from intentionally targeting US citizens in surveillance, and limits targeting foreign citizens for more than 24 hours, without acquiring a warrant. Despite this, the NSA still monitors US traffic. In fact, in 2011, the FISA court ruled that the NSA was illegally collecting US emails and had to stop. Instead, the NSA now separates US emails into separate database [1], the justification for which is that the DOD guidelines don't count data as "collected" unless it is "received for use by a DOD intelligence component [including NSA agents] in the course of their official duties." [2] Thus, according to the DOD guidelines, it's ok for the NSA to store US emails without a warrant, but they need a warrant if they want to read them.

The most rudimentary form of monitoring the government conducts is at the ISP level. There have been various programs to do this, but the most successful (and as far as we know, the one currently in use) was revealed in 2003, by AT&T technician Mark Klien. Klien reported that there was a room in the SBC communications building in San Francisco called Room 641A that was being used to monitor Internet traffic. Former senior NSA analyst William Binney claims that there are "10 or 20" of these as of 2006; Room 641A is simply part of the main system in place to monitor traffic at the ISP level. [3]

Internet traffic consists of chunks of data called packets. A packet can be thought of as a letter, consisting of: the header, which is like the envelope with the recipient's and senders addresses; and the data, which is the letter's contents. Room 641A contains equipment used for Deep Packet Inspection (DPI), which filters traffic by both the header and the data. This means that the NSA can filter traffic according to who sent it, where it's going, and what it contains. However, The spread of encryption is making DPI less useful. Encrypted traffic consists of packets where the data part can be read only by the sender and the recipient, meaning that the NSA can see only who is communicating, but not what they're communicating about.

One of the ways the NSA addresses this weakness is with a program called PRISM. PRISM involves the cooperation of as many as 100 US tech companies. [4] Instead of monitoring Internet traffic directly, the NSA gets the data from tech companies the data was sent to. Former NSA contractor Edward Snowden revealed it in July of 2013. The exact details of how the government

gathers the data is unclear, but leaked NSA slides show that PRISM involves "collection [of data] directly from the servers from these US data providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple." [5] The slide says the NSA gets data "directly from the server", which could mean a couple of things: either the NSA has direct access to the server or the company takes the data directly from their server and gives it to the NSA. Google has denied allowing the NSA direct access to its servers, saying that they "disclose user data to government in accordance with the law, and we review all such requests carefully." [6] Apple has denied ever hearing about PRISM. [6]

The NSA claims it only gathers data under PRISM and related programs on a case by case basis – a fact sheet put out by Director of National Intelligence James Clapper, in response to the leaks, claims that "Under Section 702 of FISA, the United States Government does not unilaterally obtain information from the servers of US electronic communication service providers." [7] Note that Clapper only says the NSA does not unilaterally obtain information from the servers of US electronic communication service providers. Outside the US, the NSA is much less restricted, because they are allowed to assume that traffic going in and out of foreign servers is foreign, which gives rise to another program meant to gather data directly from Internet companies, called MUSCULAR, which was also revealed in the Snowden leaks. MUSCULAR involves tapping the private international networks of these large Internet companies. Since the tapping happens overseas, there are much fewer restrictions on it, allowing the NSA to freely gather data that would be encrypted when sent to the end user – before it's encrypted. [8] Like room 641A, MUSCULAR is becoming less and less useful as tech companies start encrypting their internal communication: Google started encrypting their internal communications in November 2013, and Yahoo plans to do so by early 2014. [9]

Even though we don't have all the details, it's pretty clear the NSA is heavily invested in monitoring Internet traffic; even if they don't look at it, having the capability to gather this much data is a clear violation of our right to privacy. The right to privacy is one of the most important. It's also one of the most underappreciated – after all, why would a law-abiding citizen care if the government monitors their Internet traffic, especially, if it's in the name of stopping terrorism? Systemic encroachments on the privacy of civilians are a key aspect of oppressive governments. A government that is comfortable abusing its technical advantages to gather a complete profile of all of its citizens effectively has the ability to blackmail any of its citizens. On a less extreme scale, if the NSA has access to the private Internet history and emails of government officials, they have leverage to blackmail those officials—especially those up for election. Imagine if a the NSA threatened to publicly release embarrassing emails or browsing habits of any congressman who tried to cut their funding,

hurting their reelection chances. It's impossible to know if the NSA does this, but at this point, the NSA enforces the only regulations on the NSA. Losing the right to privacy also means losing protection for whistleblowers like Edward Snowden, who is now a fugitive from the US government. If the NSA had access to his email records, he almost certainly would have been stopped, before his leaks reached the public, only serving to further cover-up a fundamental flaw of the system as a whole.

Even if we trusted the government to protect our right to privacy in the face of growing surveillance, the government is made up of flawed individuals. The Snowden leaks detail "thousands of abuses", from mistyped search terms (one incident caused the NSA to gather thousands of phone calls from Washington DC because of a software glitch) to agents spying on love interests. [10] Officially, the NSA admits to an average of one abuse a year over the past decade. [11] These abuses are happening on a relatively small scale, but they serve to highlight an important point: the apparatus that this data is flowing into is not a perfect machine of justice, but a complex collection of people, some good, some bad, some competent, others incompetent.

Over the past decade or so, the NSA has successfully set up a very extensive Internet monitoring system. They can monitor nearly anything a person does on the Internet. They have access to browsing history through programs like room 641a, and they have direct access to emails and other data through programs like PRISM and MUSCULAR. These monitoring capabilities are not in and of themselves a problem, being able to intercept criminal's communications has always been an important part of law enforcement, and it's becoming more important with the rise of ubiquitous communication devices like cellphones and laptops, as well as the rise of virtual crime. The strategies employed by the NSA to monitor Internet traffic are troubling. The NSA has shown a clear disregard for our right to privacy and the law. Unfortunately, they did not do this alone. Congress has been complacent at best, and the judicial branch has been slow to challenge violations of the law. Now that the full extent of this surveillance is becoming clear, it's more important than ever to write your elected officials, raise awareness, and support companies that respect individual privacy.

Notes

[1] CNET News. (2013). Facts on the Collection of Intelligence Pursuant to Section 702. Retrieved October 10, 2013 from http://www.scribd.com/doc/146570400/PRISM-Facts-on-the-Collection-of-Intelligence-Pursuant-to-Section-702

[2] Department of Defense. (1982). *Procedures Governing the Activities of DOD Intelligence Components that affect United States Persons.* (DoD 5240 1-R). Retrieved December 13, 2013 from http://www.fas.org/irp/doddir/dod/d5240_1_r.pdf

[3] Bamford, J. (2012). The NSA Is Building the Country's Biggest Spy Center (Watch What You Say) . *Wired*. Retrieved October 9, 2013 from http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

[4] Gellman, B., & Poitras, L. (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program – The Washington Post.The Washington Post. Retrieved October 10, 2013 from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-Internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

[5] Ball, J. (2013). NSA's Prism surveillance program: how it works and what it can do. *The Guardian* . Retrieved October 10, 2013 from http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google

[6] Greenwald, G., & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved October 10, 2013 from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[7] CNET News (2013).

[8] Gellman, B., & Soltani, A. (2013). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. Retrieved December 15, 2013 from http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

[9] Brandon, R. (2013). The Verge. *The Verge*. Retrieved December 15, 2013 from http://www.theverge.com/2013/11/18/5118150/yahoo-ceo-marissa-mayer-plans-to-encrypt-data-against-nsa-by-2014

[10] Gellman, B. (2013). NSA broke privacy rules thousands of times per year, audit finds. *The Washington Post*. Retrieved December 14, 2013 from http://articles.washingtonpost.com/2013-08-15/world/41431831_1_washingtonpost-national-security-agency-docments

[11] Dozier, K. (2013). NSA admits rare willful surveillance violations. *Yahoo! News*. Retrieved December 15, 2013 from http://news.yahoo.com/nsa-admits-rare-willful-surveillance-violations-211422017.html